UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/667,804	09/22/2003	Linwood Hugh Overby JR.	5577-284	2160

46589 7590 12/31/2007

MYERS BIGEL SIBLEY SAJOVEC P.A.
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
TO, BAOTRAN N	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
12/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/667,804	OVERBY, LINWOOD HUGH	
	Examiner	Art Unit	
	Baotran N. To	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/01/2007(RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *2-14,16-25 and 27-31* is/are pending in the application.

4a) Of the above claim(s) *1, 15, and 26 (Canceled)* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-14,16-25 and 27-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/01/2007 has been entered.

This Office action is responsive to the Applicant's Amendment filed 09/17/2007.

Claims 2-3, 5-11, 16, 19-25, and 27-31 are amended.

Claims 1, 15, and 26 are currently canceled.

Claims 2-14, 16-25, and 27-31 remain for examination.

Response to Arguments

2. Applicant's arguments with respect to claims 22-4, 16-21, 23-25, and 27-31 have been considered but are moot in view of the new ground(s) of rejection.

Applicant argues that Aucsmith does not disclose "**selectively responding** to a notification of an intrusion" and whether the computer is protected by a firewall from a source of the intrusion" (Page 8 of Remarks).

Examiner respectfully disagrees with applicant. Aucsmith clearly discloses, "The notification may also include the server 104 notifying the client terminals 102(1)-102(N) with a message or other alert. For example, the server 104 may send a message to

the client terminals 102(1)-102(N) via electronic mail, pager, or other similar mechanism, cause a visual and/or audio notice to appear at the client terminals 102(1)-102(N), and/or take other similar actions. In addition to or instead of notifying the client terminals 102(1)-102(N) of the anomaly, the server 104 may notify 224 the firewall 112 of the anomaly. The server 104 may send this notification in real time. This notification may include updating the collection of corporate security data 120 to include information about the anomaly, modifying security procedures to account for the anomaly, or performing other similar tasks." (Paragraph 0053-0054). Furthermore, Aucsmith clearly discloses, "Once the application monitor 308 examines information it receives, the application monitor 308 may send the information through the firewall 310 to the intrusion detection mechanism 312. The firewall 310 may consult information included in a firewall collection of data 328 and/or with the control program 316 in determining whether to pass the information through the firewall 310. The intrusion detection mechanism 312 can receive information, perform any additional intrusion detection operations on the information, such as making a record of the information before sending the information to the network 108, possibly consulting an intrusion detection collection of data 330 and/or the control program 316. Information can flow between the intrusion detection mechanism 312 and a network, such as the network 108 or the VPN 114" (Paragraph 0065).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 27-31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 27-31 are directed to a computer program product for responding to an intrusion, which is defined in the specification such as "As will be appreciated by one of skill in the art, the present invention may be embodied as methods, systems, and/or computer program products. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects all generally referred to herein as a 'circuit' or 'module' (Page 4, lines 19-28). Claims 27-31 appear to read on software per se because a computer program product is implemented via software alone. Software by itself is not statutory.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 2-14, 16-25, and 27-31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 5-7, 9, 22-23, and 31 recite the limitation "**selectively responding** to a notification of an intrusion" in line 3. There is insufficient antecedent basis for this

limitation in the claim. It is unclear what applicant is intended metes and bounds of the claim language.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 5-14 and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Aucsmith et al. (U.S. Patent Application Publication 2003/0110392 A1) hereinafter Aucsmith.

Regarding Claim 5, Aucsmith discloses a method of responding to an intrusion, the method comprising:

selectively responding to at least one notification of an intrusion (paragraph 0054), from a network-accessible intrusion detection service manager (Figure 1, element 104/116, paragraph 0027), by a computer (Figure 1, element 102) evaluating the notification based on local IDS policy that includes information relating to the notification of an intrusion and information related to the computer (paragraphs 0051-0055, 0065 and 0070), wherein the information related to the computer is based on

whether the computer is protected by a firewall from a source of the intrusion (Figure 1, element 112, and Figure 3, element 310, paragraphs 0030, 0033, 0051-0055 and 0061).

Regarding Claim 22, Aucsmith discloses a computer system that responds to intrusions, the computer system comprising:

a plurality of computers (Figure 1, elements 102(1 to N)), each comprising a local IDS policy (paragraphs 0027, 0038 and 0070);

an intrusion detection service (IDS) manager (element 104/116) that is configured to generate for the computers at least one notification of an intrusion (Figure 1, paragraph 0054), and wherein each of the computers is configured to selectively respond to the notification based on the local IDS policy and information relating to the computer (paragraphs 0051-0055, 0065 and 0070) wherein at least one of the computers is configured to selectively respond to the notification based on the local IDS policy the information related to the computer is based on whether the computer is protected by a firewall from a source of the intrusion (Figure 1, element 112, and Figure 3, element 310, paragraphs 0030, 0033, 0051-0055 and 0061).

Regarding Claim 10, Aucsmith discloses the limitations of Claim 5 above. Aucsmith,further discloses downloading the local IDS policy from a network-accessible repository to the computer (paragraphs 0028, 0038 and 0083).

Regarding Claim 11, Aucsmith discloses the limitations of Claim 1 above. Aucsmith further discloses wherein the local IDS policy comprises one or more response actions to be taken based on a notification from the network-accessible IDS manager of an intrusion (paragraph 0050).

Regarding Claim 12, Aucsmith discloses the limitations of Claim 11 above. Aucsmith further discloses wherein the response action comprises terminating an application that is a target of an attack (paragraph 0037).

Regarding Claim 13, Aucsmith discloses the limitations of Claim 11 above. Aucsmith further discloses wherein the response action comprises discarding information in a communication to the computer (paragraph 0037).

Regarding Claim 14, Aucsmith discloses the limitations of Claim 11 above. Aucsmith further discloses wherein the response action comprises discontinuing communication with a source of the communication (paragraph 0039).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-4, 16-21, 23-25, and 27-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al. (U.S. Patent Application Publication 2003/0110392 A1) hereinafter Aucsmith in view of Raikar et al. (U.S. Patent Application Publication 2003/0110392 A1) hereinafter Raikar.

Regarding Claim 6, Aucsmith discloses a method of responding to an intrusion, the method comprising:

selectively responding to at least one notification of an intrusion (paragraph 0054), from a network-accessible intrusion detection service manager (Figure 1, element 104/116, paragraph 0027), by a computer (Figure 1, element 102) evaluating the notification based on local IDS policy that includes information relating to the notification of an intrusion and information related to the computer (paragraphs 0051-0055, 0065 and 0070),

Aucsmith does not explicitly disclose "wherein the information related to the computer is based on memory utilization in the computer."

However, Raikar expressly discloses wherein the information related to the computer is based on memory utilization in the computer (paragraph 0043).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Raikar's invention within Aucsmith to include wherein the information related to the computer is based on memory utilization in the computer. One of ordinary skill in the art would have been motivated to do so

because it would provide a consolidated correlation of the information (Raikar, paragraph 0008).

Regarding Claim 7, Aucsmith discloses a method of responding to an intrusion, the method comprising:

selectively responding to at least one notification of an intrusion (paragraph 0054), from a network-accessible intrusion detection service manager (Figure 1, element 104/116, paragraph 0027), by a computer (Figure 1, element 102) evaluating the notification based on local IDS policy that includes information relating to the notification of an intrusion and information related to the computer (paragraphs 0051-0055, 0065 and 0070),

Aucsmith does not explicitly disclose "wherein the information related to the computer is based on processor utilization in the computer."

However, Raikar expressly discloses wherein the information related to the computer is based on processor utilization in the computer (paragraph 0043).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Raikar's invention within Aucsmith to include wherein the information related to the computer is based on processor utilization in the computer. One of ordinary skill in the art would have been motivated to do so because it would provide a consolidated correlation of the information (Raikar, paragraph 0008).

Regarding Claim 9, Aucsmith discloses a method of responding to an intrusion, the method comprising:

selectively responding to at least one notification of an intrusion (paragraph 0054), from a network-accessible intrusion detection service manager (Figure 1, element 104/116, paragraph 0027), by a computer (Figure 1, element 102) evaluating the notification based on local IDS policy that includes information relating to the notification of an intrusion and information related to the computer (paragraphs 0051-0055, 0065 and 0070),

Aucsmith does not explicitly disclose "wherein the information related to the computer is based on proximity utilization in the computer."

However, Raikar expressly discloses wherein the information related to the computer is based on proximity utilization in the computer (paragraphs 0021 and 0043).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Raikar's invention within Aucsmith to include wherein the information related to the computer is based on proximity utilization in the computer. One of ordinary skill in the art would have been motivated to do so because it would provide a consolidated correlation of the information (Raikar, paragraph 0008).

Regarding Claims 23 and 31, Aucsmith discloses a computer system that responds to intrusions, the computer system comprising:

a plurality of computers (Figure 1, elements 102(1 to N)), each comprising a local IDS policy (paragraphs 0027, 0038 and 0070);

an intrusion detection service (IDS) manager (element 104/116) that is configured to generate for the computers at least one notification of an intrusion (Figure 1, paragraphs 0051-0055), and wherein each of the computers is configured to selectively respond to the notification based on the local IDS policy and information relating to the computer (paragraphs 0038 and 0051-0055) wherein at least one of the computers is configured to selectively respond to the notification based on the local IDS policy (paragraphs 0051-0055), and Aucsmith does not explicitly disclose "based on at least one of memory utilization in the computer and processor utilization in the computer."

However, Raikar expressly discloses based on at least one of memory utilization in the computer and processor utilization in the computer (paragraph 0043).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Raikar's invention within Aucsmith to include based on at least one of memory utilization in the computer and processor utilization in the computer. One of ordinary skill in the art would have been motivated to do so because it would provide a consolidated correlation of the information (Raikar, paragraph 0008).

Regarding Claim 2, Aucsmith and Raikar disclose the limitations of Claim 9 above. Aucsmith further discloses wherein the information related to the computer is

based on whether the computer is a firewall for other computers in the computer system (Figure 3, element 310, paragraph 0065).

Regarding Claims 3, 21 and 29, Aucsmith and Raikar disclose the limitations of Claim 9 above. Aucsmith further discloses wherein the information related to the computer is based on whether the computer is a server of information for other computers in the computer system (Figure 1, paragraphs 0025, 0033, 0037 and 0051-0055).

Regarding Claim 4, Aucsmith and Raikar disclose the limitations of Claim 3 above. Aucsmith further discloses evaluating whether the computer serves as at least one of a webserver, an intranet application server, and a backend server (paragraphs 0025 and 0027).

Regarding Claim 8, Aucsmith and Raikar disclose the limitations of Claim 6 above. Aucsmith further discloses wherein the information related to the computer is based on information from other than the IDS manager that indicates an intrusion into the computer (Figure 1, elements 116 and 120, paragraph 0026 –0028).

Regarding Claim 16, Aucsmith and Raikar disclose the limitations of Claim 15 above. Aucsmith further discloses wherein the IDS manager is configured to determine

that an intrusion has occurred in the computer system, and is configured to generate a notification based on determining that an intrusion has occurred (paragraph 0045).

Regarding Claim 17, Aucsmith and Raikar disclose the limitations of Claim 16 above. Aucsmith further discloses wherein at least two of the computers respond differently to the same intrusion notification from the IDS manager (paragraph 0055).

Regarding Claim 18, Aucsmith and Raikar disclose the limitations of Claim 16 above. Aucsmith further discloses wherein at least one of the computers responds differently to the same intrusion notification repeated at least once over time (paragraph 0055).

Regarding Claim 19, Aucsmith and Raikar disclose the limitations of Claim 15 above. Aucsmith further discloses a plurality of sensors (agents 106) that are configured to sense events that may indicate one or more possible intrusions into the computer system, and that are configured to inform the IDS manager of the events, and wherein the IDS manager is configured to determine that an intrusion has occurred in the computer system by correlating the events from the sensors (Figures 1 and 2, elements 106(1-N) and step 210, paragraphs 0035 and 0041).

Regarding Claim 24, Aucsmith and Raikar disclose the limitations of Claim 23 above. Aucsmith further discloses wherein at least one of the computers is configured

to selectively respond to the notification based on the local IDS policy and information relating to possible intrusions into the computer (paragraphs 0051-0055).

Regarding Claim 25, Aucsmith and Raikar disclose the limitations of Claim 1 above. Aucsmith further discloses wherein the information related to the computer is based on proximity of the computer to a source of the intrusion (paragraphs 0028 and 0051-0055).

Regarding Claims 20 and 27, Aucsmith and Raikar disclose the limitations of Claim 5 above. Aucsmith further discloses downloading the local IDS policy from a network-accessible repository to the computer (paragraphs 0028, 0038 and 0083).

Regarding Claim 28, Aucsmith and Raikar disclose the limitations of Claim 31 above. Aucsmith further discloses wherein the local IDS policy comprises one or more response actions to be taken based on a notification from the network-accessible IDS manager of an intrusion (paragraph 0050).

Contact Information

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BT
12/14/2007

THANHNGA TRUONG
PRIMARY EXAMINER